IT-ES7110-IM-3GS
Managed Industrial Ethernet Switch
User Manual

Statement

Copyright Notice

Information in this document is reserved by Intellisystem Technologies. Reproduction and extract without permission is prohibited.

Agreement

As the product version upgrades or other reasons, this document is subject to change without notice. Unless other agreement, this document only as a guide to use. All statement, information and suggestion in this document, without warranty of any kind, either expressed or implied.

Revision History

Version No.	Date	Reaso
V1.0.0	2014-6-11	Creating

Notes

In reading this manual, please pay attention to the following symbols,

Information necessary to explain

Special attention

Content

3

5

Chapter 1 Summarize

1.1 Introduction

IT-ES7110-IM-3GS is a industrial grade, managed and redundancy Ethernet switch. IT-ES7110-IM-3GS series provided some kinds of advanced network managed function, like as: SW-Ring redundancy ring network, VLAN, Trunking, Quality of Service, Speed control, port mirroring, fault alar m and firmware upgrade online. SW-Ring can bring your Ethernet to intelligent redundancy. Standard Industry design, can satisfied every requirement of the industry scene. All components used industry grade, it takes products high Reliability. It provided wide voltage power supply input.

SWRing™ is designed as a rapid redundancy network arithmetics. It provided recover technology for fault of rapid redundant network, the recovery time<20ms.

1.2 Features

High performance network exchange technology

- Support IEEE802.3, IEEE802.3u, IEEE 802.3x, IEEE802.1Q, IEEE802.1p, IEEE802.1D, IEEE802.1W
- SW-Ring ring network patent technology (Fault recovery time<20ms）
- Support RSTP, way exchange time<1s
- Support WEB configuration
- Support MAC address learning, aging
- automatic Support port status display, data
- update.
- Support static and dynamic IGMP
- Support flow statistics
- Support bi-directional port mirroring
- Support rate control, Broadcast storm
- control Support configuration file up and download Support 1 channel relay alarm output

Reliable Industrial grade design
- Industrial grade 4 design, -40-85℃work
- temperature No fan deign
- IP30 protection grade

CHAPTER 2 HARDWARE DESCRIPTION

2.1 Panel Design
IT-ES7110-IM-3GS-P(12/48VDC)
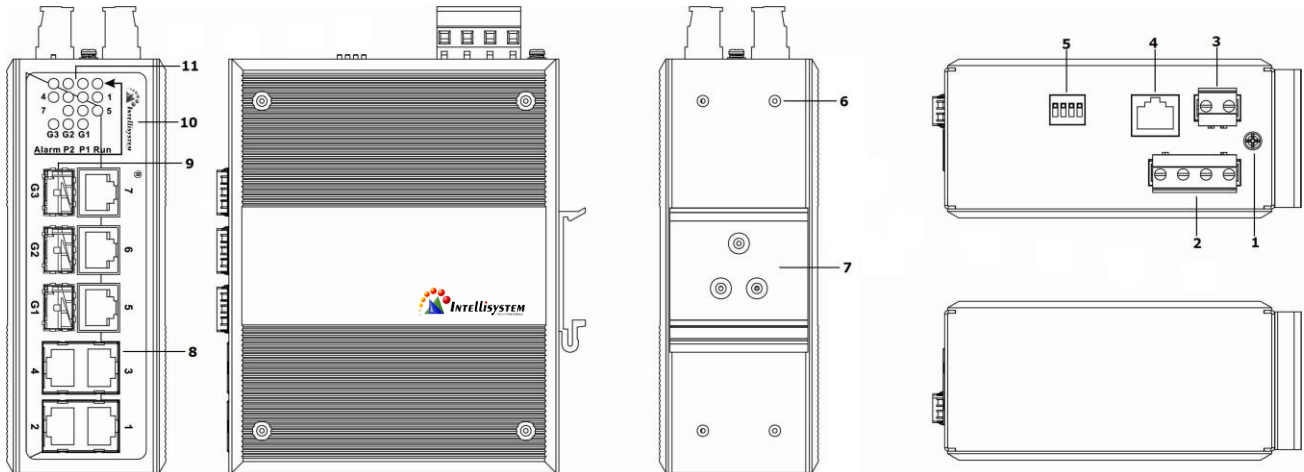
1. Ground screw
2. PWR1/PWR2 power input
3. Relay output terminal block
4. DIP switch
5. CONSOLE port
6. DIN-Rail mount
7. Wall mount screw hole
8. 10Base-T /100Base-TX port
9. Company logo, series
10. 1000Base-FX SFP port
11. LED indicator

2.2 Power supply input

Front view   **Top view**
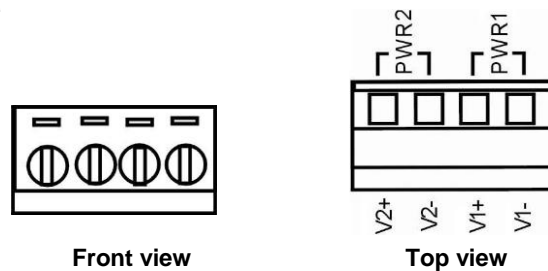
IT-ES7110-IM-3GS series top panel provided 4 bit power supply input terminal block, support DC input. DC power supply input supported redundancy function, provided PWR1 and PWR2 power input, can use for single, and can connect 2 separately power supply system, use 1 pair terminal block connect the device at the same time. If one of the power system broke, the device can work un-interruptible. built-in overcorrect protection, Reverse connection protection. Voltage input range is 12～48VDC（terminal block defined as: V1-、V1+、V2-、V2+）.

2.3 Relay connection
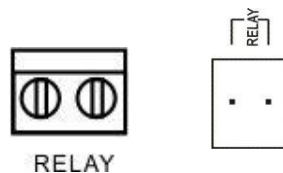
RELAY

The relay owns two contacts of the terminal block on the top pane of IT-ES7110-IM-3GS series. It is used to detect both power failure and port failure. The two wires attached to contacts form an open circuit when:

(1) IT-ES7110-IM-3GS series has lost power supply from one of the DC power inputs.
(2) One of the port is failure.

2.4 Console port

IT-ES7110-IM-3GS series provided 1pcs procedure test port based in serial port. It adopts RJ45 interface, located in top panel, can configure the CLI command through RJ45 to DB9 female cable
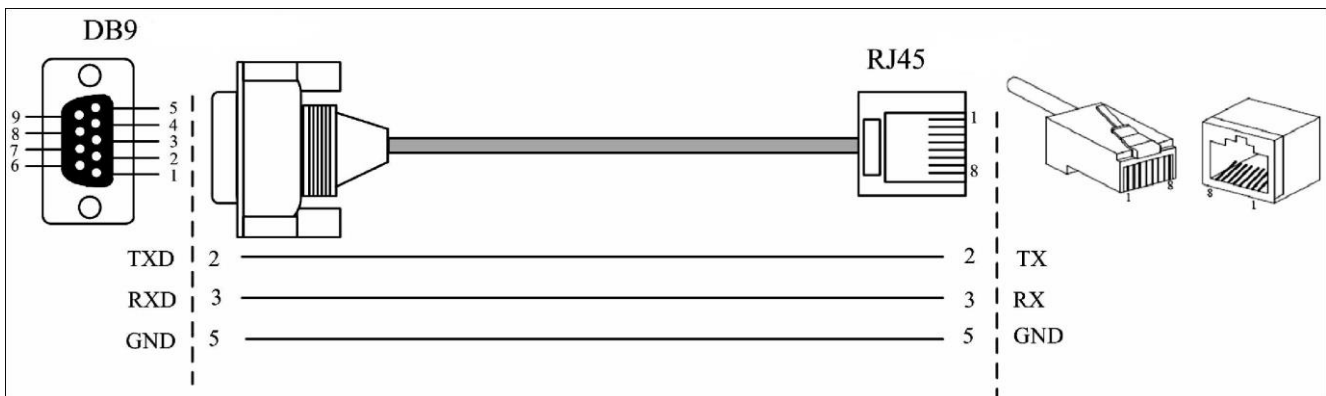
2.5 Communication port

IT-ES7110-IM-3GS series Industrial Ethernet switch provided 7 ports 10Base-T/100BaseTX（RJ45）and 3 port 1000Base-FX (SFP).

10Base-T /100Base-TX Ethernet port

10Base-T/100Base-TX Ethernet port is located on front panel and the type is RJ45. The pinout of RJ45 port connects to UTP or STP. The distance is not more than 100m. 100Mbps Ethernet connector takes 100Ωof UTP 5, 10Mbps Ethernet connector takes 100Ωof UTP 3, 4, 5.
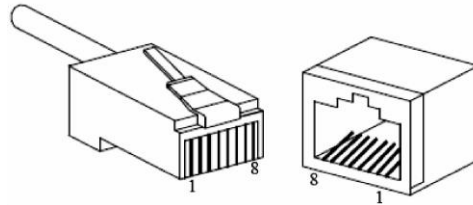
RJ 45 port supports automatically MDI/MDI-X connection. It can connect PC, Server, Converter and HUB .Corresponding connection of Pin 1,2,3,6 is like this: 1→3, 2→6, 3→1, 6→2. The definition of Pin is displayed as below.
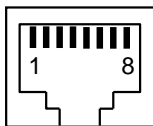
PIN	MDI	MDI-X
1	TX+	RX+
2	TX-	RX-
3	RX+	TX+
6	RX-	TX-
4, 5, 7, 8	—	—

Information necessary to explain:

Note: "TX±"Transmitting data±, "RX±"receiving data±, "—"no use

MDI（**straight-through cable**）：
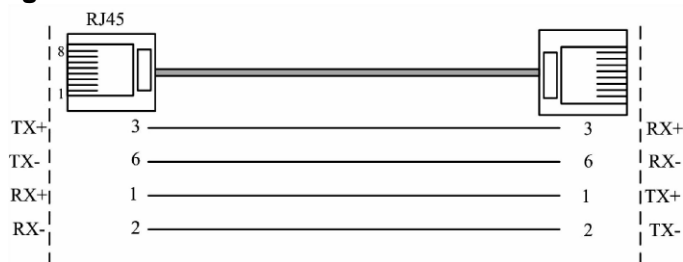
MDI-X（**Cross over cable**）：
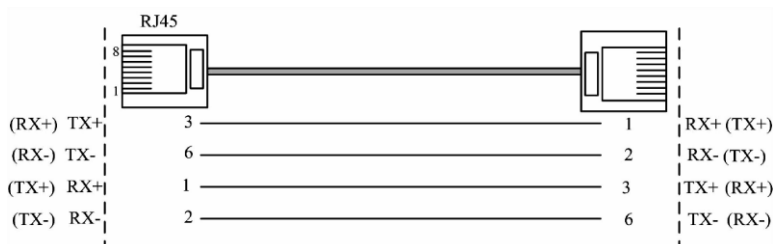
100Base-FX fiber port

100Base-FX port works with full-duplex, SM or MM SC/ST optional. The fiber port must be used in pair, TX (transmitting) port connects remote switch's RX (receive) port; RX (receiving) port connect remote

switch's TX (transmitting) port.

Suppose: If you make your own cable, we advise to label the two sides of the cable with the same letter (A-to-A and B-to-B, shown as below, or A1-to-A2 and B1-to-B2).
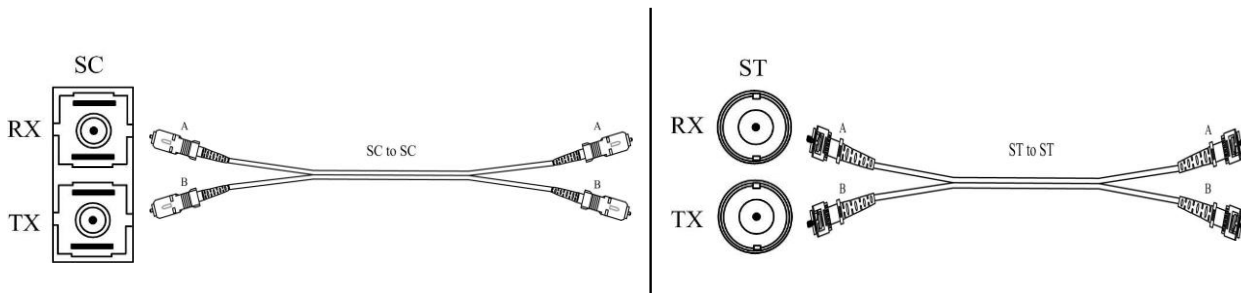
1000SFP fiber port (mini-GBIC)

1000BaseSFP fiber port adopts gigabit mini-GBIC transmission, can choice different SFP module according to different transfer distance. Fiber interface must use for pair, TX port is transmit side, must connect to RX (receive side). The fiber interface support loss line indicator.

Suppose: If you make your own cable, we suggest labeling the two sides of the same line with the same letter (A-to-A and B-to-B, shown as below, or A1-to-A2 and B1-to-B2).
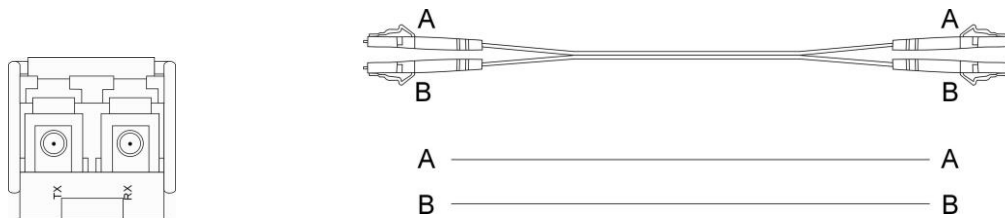
2.6 LED Indicator

IT-ES7110-IM-3GS LED indictor light on the front panel .the function of each LED is described in the table as below:

System status LED		
LED	Indicator	Description
PWR1	ON	P1 connection regularly
	OFF	P1 Power supply have no connection or unwonted
PWR2	ON	P2 connection regularly
	OFF	P2 Power supply have no connection or unwonted
Alarm	ON	Power, port have alarm
	OFF	Power, port have no alarm
Run	ON/OFF	Device unwonted
	Blinking	Device working steadily
Link/ACT（1~8/G1~G2)	ON	Established effective network connection
	Blinking	Network in activity statues
	OFF	Did not established effective network connection

2.7 Installation

Before installation, confirm that the work environment meet the installation require, including the power needs and abundant space. Whether it is close to the connection equipment and other equipment are prepared or not.

1. Avoid in the sunshine, keep away from the heat fountainhead or the area where in intense EMI.
2. Examine the cables and plugs that installation requirements.
3. Examine whether the cables be seemly or not (less than 100m) according to reasonable scheme.
4. Screw, nut, tool provide by yourself.
5. Power: redundant 12-48VDC power input
6. Environment：working temperature -40～85℃

Relative humidity 5%～95%

DIN-Rail Installation

In order to use in industrial environments expediently, IT-ES7110-IM-3GS adopts 35mm DIN- Rail installation, the installation steps as follows:

1. Examine the DIN-Rail attachment
2. Examine DIN Rail is firm or not and the position is suitable or not.
3. Insert the top of the DIN-Rail into the slot just below the stiff metal spring. 4.The DIN-Rail attachment unit will snap into place as shown below.
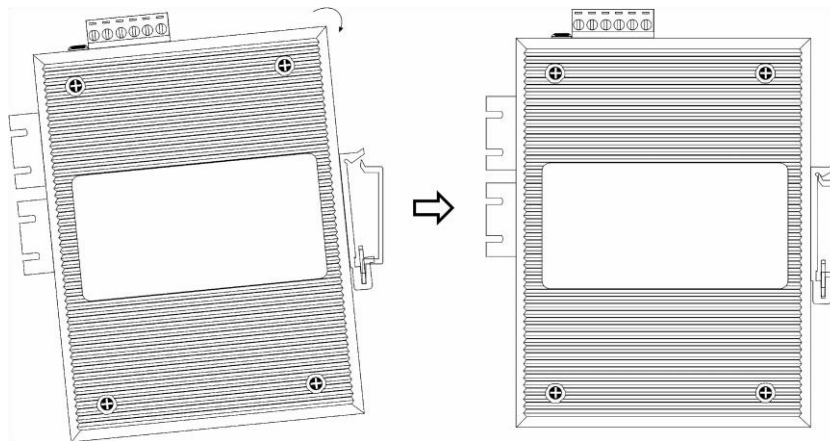
Wiring Requirements

Cable laying need to meet the following requirements,

1. It is needed to check whether the type, quantity and specification of cable match the requirement before cable laying;

2. It is needed to check the cable is damaged or not, factory records and quality assurance booklet before cable laying;

3. The required cable specification, quantity, direction and laying position need to match construction requirements, and cable length depends on actual position;

4. All the cable cannot have break-down and terminal in the middle;

5. Cables should be straight in the hallways and turning;

6. Cable should be straight in the groove, and cannot beyond the groove in case of holding back the inlet and outlet holes. Cables should be banded and fixed when they are out of the groove;

7. User cable should be separated from the power lines. Cables, power lines and grounding lines cannot be overlapped and mixed when they are in the same groove road. When cable is too long, it cannot hold down other cable, but structure in the middle of alignment rack;

8. Pigtail cannot be tied and swerved as less as possible. Swerving radius cannot be too small (small swerving causes terrible loss of link). Its banding should be moderate, not too tight, and should be separated from other cables;

9. It should have corresponding simple signal at both sides of the cable for maintaining.

Chapter 3 Appearance and Dimensions

3.1 Appearance

IT-ES7110-IM-3GS（12/48VDC）

13

3.2 Dimensions

138.00

53.00

110.00
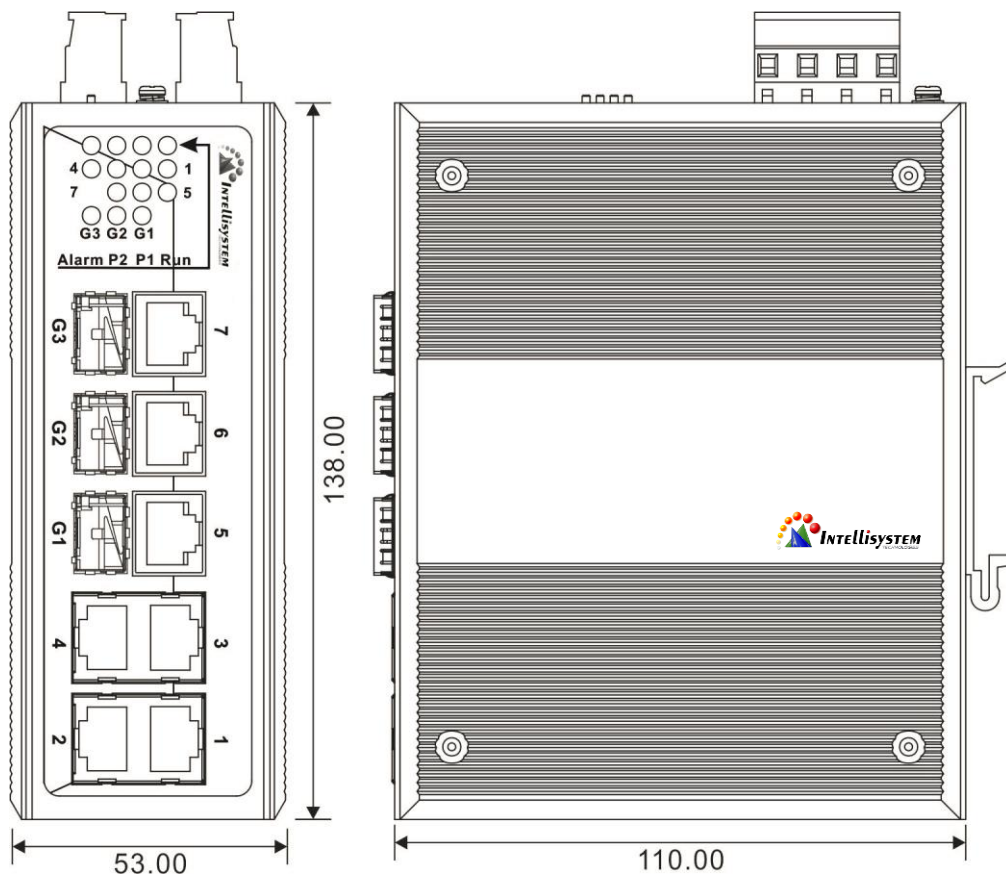
CHAPTER 4 PACKLING LIST

Please check the packaging and accessories by your first using. Please inform us or our distributor if your equipments have been damaged or lost any accessories, we will try our best to satisfy you.

Description	Quantity
Intellisystem Technologies Industrial Ethernet switch	1
User manual	1
CD	1
Warranty card	1

CHAPTER 5 NETWORK CONFIGURATION

IT-ES7110-IM-3GS can access, configuration and management through WEB, the user manual will introduce the operations step by step.

5.1 Configure PC's IP Address

IT-ES7110-IM-3GS default address is: 192.168.1.254, subnet mask is: 255.255.255.0. When entering into

IT-S7110-IM-3GS series Web interface through internet explorer, the IP address of IT-ES7110-IM-3GS series and PC must be in the same Local Area Network.

You can modify PC's or IT-ES7110-IM-3GS series's IP address to make sure that they are in the same Local Area Network. Operating process can follow method 1 or method 2 as below,

Method 1: Modify PC's IP address

➢ Click Start->Control panel->network connections->Local area Connection->Properties->Internet protocol
（TCP/IP）Setting PC's IP address: 192.168.1.X (X is less than 254, from 2 to 253).

➢ Click "OK", IP address modifies successfully
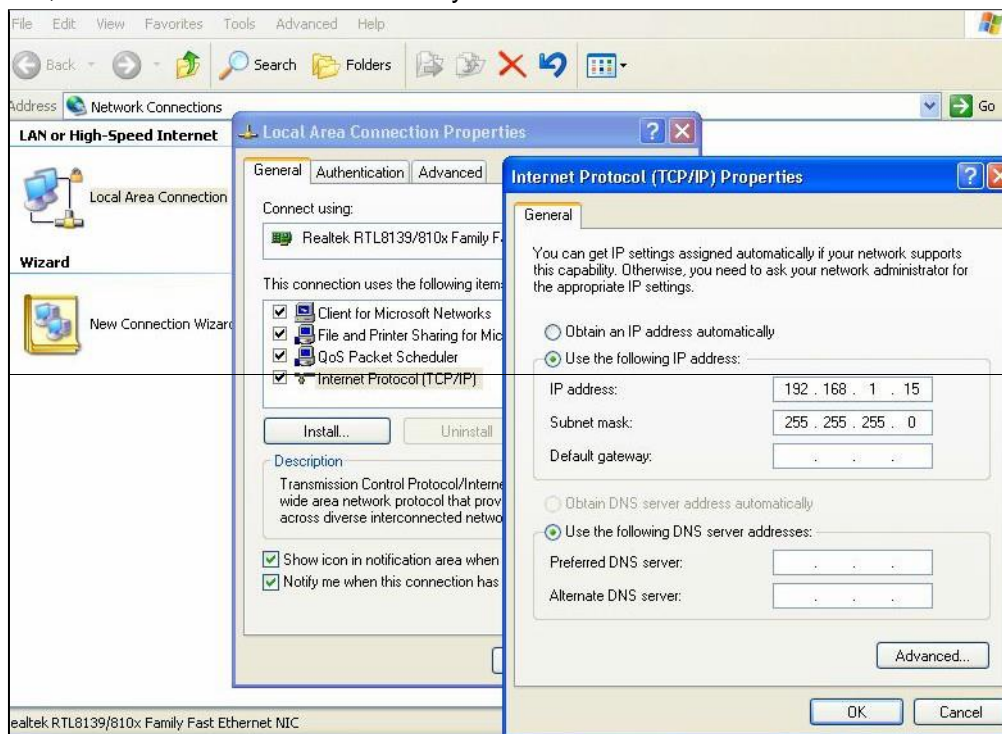
Method 2: Modify IT-ES7110-IM-3GS series's IP address through the management software.

➢ Install the management software on the PC.

➢ Enter into the management software interface, click "Search" to search the device.

➢ After searching the device, move mouse to the device, click right key, modify the device's IP address, Please make sure the device and PC in the same Local Area Network.

⚠️

This configuration example does not use the Advanced button in the last picture. In one and the same network card allows the use of multiple IP pseudo-address when use the advanced configuration of the IP address, at which does not change the original address can still access the switch device. But in the IGMP polling and IEEE 802.1x polling windows system can not handle correctly, Unix-like system does not have this problem. The advanced users have to pay attention to this issue.

CHAPTER 6 WEB MANAGEMENT

IT-ES7110-IM-3GS series have WEB server inside, can manage and maintenance the device very intuitive through WEB interface

6.1 Configurate preparing

1. The lowest requirement for user's computer is as below:
◆   Install operating system (Windows XP/2000,etc)
◆   Install Ethernet card
◆   Install Web explorer (IE6.0 or higher version)
◆   Install and start TCP/IP protocol

2. Establish the correct network configuration
The default management IP address of IT-ES7110-IM-3GS series: 192.168.1.254, subnet mask as: 255.255.255.0. Before access to the configuration interface, the computer's IP address and the switch must be configured in the same subnet (IP address configuration,please refer to "5.1") if need local configuration; Computers and switches must be routed reach if for remote configuration.

How to log on to Web Server
Please type in the default IP of switch on the browsers's address bar, and then will pop-up a window by clicking the "enter" key which shows you have to enter your user name and password. The default username and password is "admin". You can enter your username and password 3 times if you found the username and password is incorrect.If the 3 input error, the browser will display a "401 Unauthorized" error message. Refresh the page and then enter the correct user name and password, log on to the Web Server, it will recommend to modify the user name and password.Please contact our customer service center if you have more questions.

(Figure 6.1.1)

The default username and password is [admin], case sensitive for this series. The default password is with administrator privileges.

Menu Introduction:

Main Menu	Tag	Function
System Status	System information	Display device information and port information such as software version, IP address, etc.
Port Configuration	Port settings	Display and configure information of each port: such as connection status, configuration modes, flow status etc.
	Bandwidth management	Set the maximum rate of the input/output packets for port.
L2 feature	VLAN	Displays the current list of 802.1Q VLAN, configure and manage 802.1Q VLAN.
	IGMP snooping	Display port-based VLAN list, and to configure and manage port- based VLAN.
	Static Multicast	Configure the static multicast MAC address and its corresponding port.
QOS	QoS classification	Configure the the QOS queue mode, QOS implementation and port default priority.
	Cos Mapping	Configure the meaning of COS value.
	Dscp	Configure the DSCP priority.
Redundancy	Port Trunking	Configure port trunking group.
	Rapid Ring	Configure the rapid ring network port and type.
	RSTP	Configure the parameters of RSTP.
Access	Login Settings	Configure different permissions for the user name and
Remote Monitoring	SNMP	
	Relay Warning	
Port Statistics	Frame statistics	
Diagnosis	Mirror	Configure the mirror port and mirrored port.
Basic Settings	System Identification	Device IP, gateway, DNS and other information.
	System Log	Log information.
	System File update	Software upgrade, acquire, preserve or restore the switch configuration.

Web Timeout Treatment

The system timeout will cancel the login if the user did not login for a long time (The configuration of this login will be remained in the Web interface).

If user doesn't operate the Web interface for a long time, The system will be canceled this login.(but configuration change made in this login will be saved in Web configuration interface.). If the user wants to do any operating on Web configuration interface again, the system will remind user and returns to the login dialog box. Users need to log in again if operating is needed. The timeout time is 300s.

6.2 System status

Device information

Current Location>>Main Menu>>System Status>>Overview

Device Information

Name :	IndustrialSwitch	Hardware Ver :	V2.0.0
Module :	MangedSwitch	Firmware Ver :	1.1.0 build201405061R
Description :	10PORT		
Serial No. :		Contact Information :	

Figure 6.2.1

Configuration Items	Description
Name	Network mark of the device. It is convenient for management tools to judge.
Serial No.	Serial number of the device. It is convenient for device management.
Description	Description of the product features.
Contact Information	Contact information of the operator for device maintenance.
MAC address	Hardware address of the device. It is an unique address which is made up of hexadecimal number with 48 bits (6 bytes) in length.
Hardware Version	Current hardware version.
Firmware Version	Current firmware version.
Current Time	Current time of the device.
Run Time	Run time after the device is powered on. When the device reboots, the time need to recalculate.

Time display

Current Time : Thu May 29 10:04:58 UTC+0800 2014
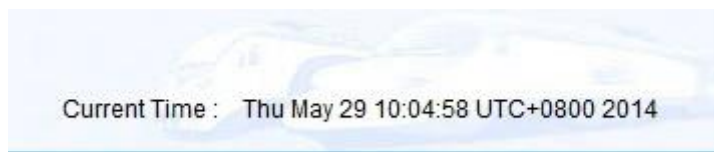
（Figure 6.2.2）

Port	Connection	Duplex	Speed	Type
1	LOS	HALF	10M	TX
2	LOS	HALF	10M	TX
3	LOS	HALF	10M	TX
4	LINK	FULL	100M	TX
5	LOS	HALF	10M	TX
6	LOS	HALF	10M	TX
7	LOS	HALF	10M	TX
G1	LOS	FULL	1000M	FX
G2	LOS	FULL	1000M	FX
G3	LOS	FULL	1000M	FX

（Figure 6.2.3）

Port 3，7...G1，if the port is connected properly the status should be LINK, no connection status will be LOS.

6.3 Port Configuration

6.3.1 Port Settings

The port configuration interface mainly include port type (Electric port or optical port), setup speed mode and duplex mode,flow control. Only when the port is enabled for the port speed, duplex, flow control will work. Select auto-negotiation, speed, duplex auto-negotiation.

（Figure 6.3.1）

Configuration Items	Description
Port	Port name, corresponding to mark in panel.
Type	Display port type (TX or FX).
Speed	Display configurable speed of port or auto-negotiation mode.
Duplex	Auto-negotiation（AUTO）,full duplex（FULL）, half duplex（HALF） optional, default mode is auto-negotiation mode.
Enable	Configurable port enable or disable. Selecting square frame is for enable the corresponding port. It can not transmit data if any port disable. The default is "Enable".
Flow Control	Whether selecting flow control to the port. Only can selecting flow control when the port enable. The default is off.

The described Electric port is the common network device RJ-45 port, commonly known as "crystal head", it's is a twisted-pair Ethernet interface type. This interface can be used in 10Base-T, 100Base-Tx and 1000Base-Tx Ethernet, transmission media is twisted pair, but according to different bandwidth media have different requirements, in particular, 1000Base-Tx Gigabit Ethernet connection, at least to use cat5e.

Port Speed
Port speed shows the connecting speed of the port. It includes 3 kinds of speed: 10M, 100M and auto-negotiation. 10M uses 10base-T standard and UTP cable for connection. When the port is in 10M speed, Link/Act indicator will blink continuously while data transmitting and status indicator of 10M/100Mbps will stay OFF.
100M uses 100Base-TX standard and UTP/STP cable for connection. When the port is in 100M speed,

Link/Act indicator will blink continuously while data transmitting. 100M fiber port uses 100Base-FX standard and single/multi-mode fiber for connection. Main fiber of 100Base-FX standard includes: 62.5nm multi-mode fiber and 50nm multi-mode fiber.Auto-negotiation includes 2 kinds of speed according the capability of the other end: 10M and 100M.

Port Enable

This item provides a device to enable/disable the port. When choosing disable, the device would cut off power supply of this port. Even if other device is connected to this port, all status indicators of this port are OFF. Only enable this port, all settings about this port will be valid. This item provides a kind of safety mechanism to protect the port from illegal use. It is not allowed to disable all the ports.

Duplx Mode

Full duplex of the switch means switch can transmit and receive data at the same time. Half duplex of the switch means switch can transmit or receive data in a certain time. Generally the speed will choose auto- negotiation so that the port can automatically judge the connection type of the device connected to it and automatically adjust the connection type to ensure the maximum compatibility.

Flow Control

Flow control is used to prevent the frames from discard while port is blocked. This method is to send back the blocking signal to its original address while sending or receiving buffer area start to overflow. It limits the abnormal flows into a certain range. Flow control can be effective in preventing large amounts of data in the network instant impact on the network to ensure the efficient and stable user network running.

Two types of flow control:

1. In the half duplex mode, flow control is through back pressure. It is to send a jamming signal to the transmission source to reduce transmission speed.

2. In the full duplex mode, flow control generally follow IEEE 802.3x standard. Switch sends "pause" to information source to pause its sending information.

Use flow control to control the data flow between the sending and receiving nodes, can prevent packet loss.

Polarity (MDI/MDIX auto-negotiation)

MDI-II (Medium Dependent Interface- II mode), is a kind of standard built by IEEE for RJ-45 UTP cable of fast Ethernet 100BASE-T. II stands for parallel configuration. MDI-X(Media Dependent Interface-x mode) 与 MDI- II is a kind of standard built by IEEE for RJ-45 UTP cable of fast Ethernet 100BASE-T. X stands for crossover configuration.

6.3.2 Bandwidth Management

Bandwidth management mainly refers to limit the data's egress and ingress bandwidth to save the network sources.

Click [port setting/bandwidth management] and enter into the following interface.

Egress Bandwidth Configuration:

"No limit" stands for no limitation for the speed, the others are corresponding speed.

As shown in following figure 6.3.2, the forcible egress rate of Port 5 is 8Mbps. Only need to select 8Mbps in egress rate setting of Port 5. The bandwidth of Port 5 as receiver is still 100Mbps, but the forcible egress bandwidth of Port 5 is 8Mbps.

Egress

Port	Rate	Port	Rate	Port	Rate	Port	Rate	Port	Rate
1	No Limit ▾	2	No Limit ▾	3	No Limit ▾	4	No Limit ▾	5	8M ▾
6	No Limit ▾	7	No Limit ▾	G1	No Limit ▾	G2	No Limit ▾	G3	No Limit ▾

Ingress

Ingress Bandwidth Configuration:
Ingress bandwidth limit includes 4 kinds: 1 All frames;
2 Broadcast&Multicast &unicast frames; 3 Broadcast&Multicast only;
4 Broadcast only

"No limit" stands for no limitation, the rate of low priority queues（L）can be setted:128k, 256k, 512k, 1M, 2M, 4M, 8M.The rate of normal priority queues（N）is 1 or 2 times as wide as that of low priority queues. The rate of medium priority queues（M）is 1 or 2 times as wide as that of normal one. The rate of high priority queues is 1 or 2 times as wide as that of medium one.

For example, the rate of low priority queues is 256k, then the rate of normal priority queues can be set for 256k or 512k. Detailed operating as shown in Figure 6.3.3 and Figure 6.3.4

Port	Policy	Rate of Low Priority Queue	Rate of Normal Priority Queue	Rate of Medium Priority Queue	Rate of High Priority Queue
1	Broadcast only	256K	256K	512K	512K
2	Broadcast only	2M	2M	2M	2M
3	Broadcast only	512K	1M	2M	2M
4	Broadcast only	8M	16M	32M	64M
5	Broadcast only	No Limited	No Limited	No Limited	No Limited
6	Broadcast only	No Limited	No Limited	No Limited	No Limited

（Figure 6.3.3）

G1	Broadcast only	32M	64M	128M	256M
G2	Broadcast only	64M	128M	256M	512M
G3	Broadcast only	256M	512M	1G	1G

Note :

The Rate of Low Priority Queue can be set to 128K,256K,512K,1M,2M,4M,8M.
The Rate of Normal Priority Queue is one time or two times Rate of Low Priority Queue.
The Rate of Medium Priority Queue is one time or two times Rate of Normal Priority Queue.
The Rate of High Priority Queue is one time or two times Rate of Medium Priority Queue.

Apply   Cancel

（Figure 6.3.4）

	Type	Low	Norm	Medium	High
Type	**All frames**	----			
	Broadcast, Multicast or unicast frames				
	Broadcast&Multicast only				

The ingress rate is related to CoS priority. Priority Queue is based on QoS setting (the same as QoS assorted setting includes checking CoS priority), or ingress rate will be based on default. CoS priority includes 4 queues:Low，Normal，Medium，High.

Operation method:

1. Choice 2 port at first, for example open the COS priority of port 4 and port 5, please according to 6.5 part
2. Then set port 4's CoS is High, port 5's CoS is LOW in COS mapping setting interface
3. Last, set the type of limit package and bandwidth of priority queue in Ingress bandwidth configuration

For example, keep up step 1 and 2, choice "All frame" in port 4 and 5 at step 3. Set 2M in all low priority queue

⚠ :

If priority queue bandwidth configuration is available, must mark the enter into port's data pack as CoS.

6.4 L2 Features

1. **VLAN**

VLAN（Virtual Local Area Network）is a kind of new data exchange technology for logically dividing LAN into many segments and making many virtual work groups. This technology mainly allows that switch can limit broadcast when LAN interconnects. This technology can divide a LAN into several logical LAN——VLAN.
Each VLAN is a broadcast domain and hosts in VLAN can communicate just like in the same LAN.But it can not interconnect between VLAN. So broadcast message is limited in VLAN.

◎Advantage of VLAN

Main advantage of VLAN is providing a network segmentation system which is more flexible than traditional network. VLAN can be divided into several broadcast domain which can restrain broadcast storm. Other advantages of VLAN are as follows:

VLAN takes convenience for devices' relocation in network. In traditional network, manager need to take so much time in moving and change of devices. If user transfers to different subnet, it needs to change each terminal's address by hand. But in VLAN, if a terminal from VLAN need to be transferred to another network, it only need to indicate that new port without new wiring.

VLAN provides higher safety features: devices can communicate with other devices from the same VLAN only.

IT-ES7110-IM-3GS switch supports based on 802.1Q VLAN. It deals with messages based on Tag of recognized message （including 802.1p priority and VLAN ID, etc.）.

Frames with 802.1q add 4 byte Tag based on Ethernet frames, including 2 byte TPID, 3 byte Priority, 1 byte CFI and 12 byte VLAN ID.

	VLAN Tag			
DA&SA	TPID	Priority	CFI	VLAN ID	Type
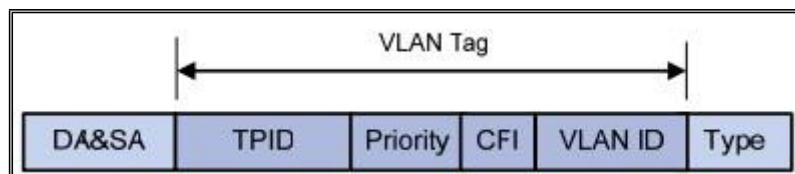
frame   16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged

.
TPID: Priority: It indicates the frame priority level. Values are from 0 (best effort) to 7 (highest); 1
a   represents

the lowest priority.

CFI: a 1-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format.

VLAN ID: a 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLAN.

◎Work mode of port

In using VLAN, each port of switch can work in different mode. There are 2 kinds of work mode for this series of switch: ACCESS mode and TRUNK mode.

Definition of VLAN functions are as follows: PVID:

Port Vlan ID.

TAG: VLAN Tag.

VLAN item: VID and its members

Access mode:

◆ Exchange port under Access mode usually belongs to a VLAN as the port connecting PC.;
◆ After Access port of switch receives Ethernet frames, it adds VLAN Tag based on port's PVID, (if Ethernet frames with VLAN Tag, then cover it); it depends on VLAN item whether adding VLAN Tag when Ethernet frames send out from Access port.
◆ Trunk mode:
➢ Exchange port under Trunk mode can belong to several VLAN. It can send and receive several VLAN data message. It is usually used on uplink port between switches.

After Trunk port of switch receives Ethernet frames, it needs to judge whether this Ethernet frames takes with VLAN Tag. If so, then don't change the VLAN Tag. If not, then add VLAN Tag of this port and transfer. It depends on VLAN item whether frames takes with VLAN Tag when it send out from Trunk port.

◎VLAN Operating Method

Enter into VLAN configuration interface, according to configuration purpose, firstly select port type. There are 2 kinds including Access and Trunk. Then set up PVID, finally add VID and its members based on PVID. In VLAN items, the members include Unmodified, Untagged, Tagged and "---" optional.

Unmodified: refers to this port is VLAN member, the frames cannot be modified when sending out; UnTagged: refers to this port is VLAN member, the frames are without Tag when sending out; Tagged: refers to this port is VLAN member, the frames need to add Tag when sending out; "---" : refers to this port is not VLAN member;

Steps for creating VLAN are as follows:
1. Enter into VLAN configuration interface, firstly select port type, Access or Trunk;
2. Enter default PVID of this port in [PVID] textbox ;
3. Enter appointed VLAN into [VID] textbox;
4. Set up members' type of each port, like Unmodified, Untagged, Tagged
5. Click [Add] button, add VLAN items into list and click [Apply] and reboot the device at last. Creating new VLAN is finished.

Steps for modifying VLAN are as follows:

This can re-configure existing VLAN including modifying member's type and quantity of the port. Steps are as follows:
1. Enter into VLAN configuration interface, firstly select VLAN items which need to modify in VLAN item list, like VLAN 1;
2. Member's type of VLAN1 shows in current VLAN item setting and set up member's type of the port according to the steps for creating new VLAN.
3. Click [Add] button, select [OK] when reminds whether overwrite it as shown in Figure6.4.1. Add new VLAN items into list and click[Apply] and reboot the device at last. Modifying VLAN finishes.

（Figure 6.4.1）

Steps for remove VLAN are as follows:

This can remove existing VLAN and steps are as follows:

1. Firstly select VLAN items which need to remove, like VLAN2;
2. After selecting, click [Delete], then [Apply]. As shown in Figure 6.4.2:

（Figure 6.4.2）

Default VLAN of IT-ES7110-IM-3GS:

A new or a restoring factory setting of IT-ES7110-IM-3GS Ethernet switch includes a VLAN, namely default VLAN, as shown in figure 6.4.3.

Definition of default VLAN is as follows:

1. PVID of all ports is 1.
2. All port type is Access.
3. All ports are located in this VLAN.

Typical VLAN configuration：

Suppose Port 3,4,5 can meet following needs, Port 3 can intercommunicate with Port5, Port4 can intercommunicate with Port5, Port3 can's intercommunicate with Port4, what will you do for VLAN？ （regardless of VLAN setting of other ports）

We can do following analysis, Port 3 can intercommunicate Port 5, their ports must belongs to a VLAN, Port4 can intercommunicate with Port5, Port4 and Port5 must belongs to a same VLAN, Port3

and Port4 belong to different VLAN. As shown in Figure6.4.4 and 6.4.5;

1. Port3's PVID is 2. Port4's PVID is 3. Port5's PVID is 4, port types are Access.
2. Add VLAN2, VLAN3, VLAN4, its members are 3 and 5, 4 and 5, 3, 4 and 5. Member types are Untagged.

VLAN Port Settings

Port :	Port CPU	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port G1	Port G2
Type :	Access	Access	Access	Access	Access	Access	Access	Access	Access	Access
PVID :	1	1	1	2	3	4	1	1	1	1

（Figure 6.4.4）

Port :	Port CPU	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port G1
VID:1	UnTagged	UnTagged	UnTagged	--	--	--	--	--	Tagged
VID:2	--	--	--	UnTagged	--	UnTagged	--	--	--
VID:3	--	--	--	--	UnTagged	UnTagged	--	--	--
VID:4	--	--	--	UnTagged	UnTagged	UnTagged	--	--	--

（Figure 6.4.5）

VLAN Configuration of Single Ring:

1. It must configure a Console port for the device. Console port and CPU port must be in the same VLAN, and Port 1 in following figure is Console port.

2. Port type of ring port must be Trunk and Tagged. As shown in Figure 6.4.6 and 6.4.7;

（Figure 6.4.6）

（Figure 6.4.7）

1.	Maximum VLAN items of IT-ES7110-IM-3GS series switch is 64, VID's value range is 1~4094. Console port refers to the port to manage and configure switch. CPU port and console port must be in the same VLAN.
2.	Propose to configure one or more port used as console port which and CPU port must be in the same VLAN. To separate console port from CPU port can prevent that CPU send managed data packets to each port to influence the communication.
3.	After configuring VLAN, it is needed to save this configuration, and reboot the switch.

6.4.2 IGMP snooping

IP host applies to join (or leave) multicast group to the neighboring router through IGMP (Internet Group Management Protocol) protocol. IGMP Snooping is multicast constraining mechanism. It manages and controls multicast group by snooping and analysis of the IGMP messages between the host and the multicast device.

Work process of IGMP Snooping: the switch snoops messages between the host computer and the router and tracks multicast information and the port applied for. When the switch snoops IGMP Report message sent from the host computer to the router, the switch would add this port to multicast forwarding list; when the switch snoops IGMP Leave message sent by the host computer, the router will send Group-Specific Query message of this port. If other hosts need this multicast, then the rely IGMP Report message. If the router doesn't get any reply from the hosts, the switch would delete this port from the multicast forwarding list. The router will send IGMP Query message regularly, the switch will deletes the port from the multicast forwarding list if it doesn't get the IGMP Report message from the host.

IGMP Snooping: Enable or disable IGMP snooping function
IGMP Query: Enable or disable IGMP query function
IGMP Query Interval: after enabling IGMP Query, the interval to check existing multicast members.
MAX Age: the maximum existing time of the members

IGMP Snooping :   ◉ Enable   ○ Disable

IGMP Query :   ◉ Enable   ○ Disable

IGMP Query Interval :   125   S (Range : 60~1000)

```
 - - - No - - - - MAC Address - - - - Type - - - - - - - Join Port - - - - - - - - - - - - - - - -
       1      01-00-5E-00-00-FC    Dynamic        4
```

（Figure 6.4.
8）

1. Must configure the VLAN of 802.1q at first, then open IGMP Snooping function
2. Please do not open more IGMP snooping, waste source.

6.4.3 Static Multicast FWD

The device provides the function of static MAC address forwarding. The destination address includes the data packets with static MAC address which will be transferred to the appointed port. Embedded forwarding address list in the switch chip can learn and support 2,000 MAC addresses and 16 multicast forwarding ports list. Static MAC address carry out transmit function, it did not accept the arrangement of aging.

Current Location>>Main Menu>>L2 Feature>>Multicast Configuration>>Static Multicast

Add New Static Multicast MAC Address to the List

MAC Address :   [   ] (XX-XX-XX-XX-XX-XX)

Join Port :   1-☐ 2-☐ 3-☐ 4-☐ 5-☐ 6-☐ 7-☐ 8-☐ G1-☐ G2-☐

Operation :   [Add]   [Delete]   [Apply]

```
 - - - - MAC Address - - - - - - - - - - - Join Port - - - - - - - - - - -
                                  1  2  3  4
```

（Figure
6.4.9）

Button [Add/Edit], [Delete] were used for add/delete static Multicast MAC address. Join port is used to choice the transmit port of static MAC address, can point to 1 or more transmit port. Knock [Add], [Delete], static MAC address will be updated. For example, add MAC address "01-00-00-00-

00-01-01" member is port 1, 2，3，4. Multicast MAC address is 1 of highest byte's low byte. All none multicast address did not allow to add

in this table and the format must according to XX-XX-XX-XX-XX-XX, did not have space or other illegal character, otherwise, will be display warning information.

1. This function has great impact on forwarding multicast, unless you can make sure the address is no problem, otherwise, please use it with caution.
2. The following multicast addresses are reserved for the device or protocol, please don't use them: 0180C20000xx, 01005E0000xx.
3. IGMP dynamic learning will not update the multicast address, static multicast forwarding is a kind of safety mechanism.

6.5 QOS

6.5.1 QOS Classification

QoS provides four internal queues, each queue supports four different levels of traffic, shorter persistence time of high-priority data packets in the switch, supports lower latency for certain delay-sensitive traffic.

According to port ID, MAC address, 802.1p priority tags, DiONetServ and IP TOS, equipment can be abale to put the packets to an appropriate level.

Qos Classification			
Queuing Mechanism :	Weighted Fair(8:4:2:1) ⌄		
	Weighted Fair(8:4:2:1)		
	Strict(High Priority First Always)		
Port	Inspect ToS	Inspect CoS	Default Port Priority
1	☐	☐	0 ⌄
2	☐	☐	0 ⌄
3	☐	☐	0 ⌄
4	☐	☐	0 ⌄
5	☐	☐	0 ⌄
6	☐	☐	0 ⌄
7	☐	☐	0 ⌄
G1	☐	☐	0 ⌄
G2	☐	☐	0 ⌄
G3	☐	☐	0 ⌄
	Apply	Cancel	

users can select the QOS priority queue mechanism, the queue mechanism in two ways: weighted Fair mode and strict mode.

6.5.2 COS

IEEE P802.1p is the name of a task group active during 1995–98 responsible for adding

traffic class expediting and dynamic multicast filtering to the IEEE 802.1D standard. Essentially, they provided a mechanism for implementing Quality of Service (QoS) at the media access control (MAC) level. The group's work with the new priority classes and Generic Attribute Registration Protocol (GARP) was not published separately but was incorporated into a major revision of the standard, IEEE 802.1D-1998. It also required a short amendment extending the frame size of the

Ethernet standard by four bytes which was published as IEEE 802.3ac in 1998.

The QoS technique developed by the working group, also known as class of service (CoS), is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value of between 0 and 7 inclusive that can be used by QoS disciplines to differentiate traffic. Although this technique is commonly referred to as *IEEE 802.1p*, there is no standard or amendment by that name published by the IEEE. Rather the technique is incorporated into IEEE 802.1Q standard which specifies the tag inserted into an Ethernet frame.

Priority levels

Eight different classes of service are available as expressed through the 3-bit PCP field in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE however has made some broad recommendations:

PCP	Priority	Acronym	Traffic Types
1	0 (lowest)	BK	Background
0	1	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Critical Applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork Control
7	7 (highest)	NC	Network Control

Current Location>>Main Menu>>QoS>>CoS Mapping

Mapping Table of CoS Value and Priority Queues

CoS	0	1	2	3
Priority Queue	Low	Low	Normal	Normal

CoS	4	5	6	7
Priority Queue	Medium	Medium	High	High

Apply   Cancel

6.5.3 DSCP

DiffServ architecture provides each transport packets in the network are classified into different categories, classified information is contained in the IP packet header, DiffServ architecture using the first 6 bits of IP packet header TOS(Type of Service) to carry the packets' classified information. This

definition is only for the lower 6 bits, one number does not exceed 63. This definition supports both IPv4 (ToS field) and IPv6 (Traffic Class field). DSCP has 64 priority values (0-63), the lowest priority 0 and the highest priority 63. In fact, the

DSCP field is a superset of the IP precedence field, DSCP field definition is backward-compatible with IP precedence field.

So far, the defined DSCP with default DSCP, the value is 0; class selector DSCP defined as the backward-compatible with IP precedence, the value(8,16,24,32,40,48,56); Expedited Forwarding (EF), generally used for low latency service, the recommended value is 46 (101110); identified by forwarding (AF) defines four service levels, each service level has 3 down process, so spent 12 DSCP values ((10,12,14), (18,20,22), (26,28,30), (34,36,38)).

The priority value of the device (1-16) is defined as the lowest priority, as the first queue. Priority value (17-32) is defined as the second queue, the priority value (33-48) is defined as the third queue, the priority value (49-64 is defined as the fastest queue, the highest priority.

Current Location>>Main Menu>>QoS>>ToS/DiffServ Mapping

Mapping Table of ToS (DSCP) Value and Priority Queues

ToS(DSCP)	Level	ToS(DSCP)	Level	ToS(DSCP)	Level	ToS(DSCP)	Level
0x00(01)	Low	0x04(02)	Low	0x08(03)	Low	0x0C(04)	Low
0x10(05)	Low	0x14(06)	Low	0x18(07)	Low	0x1C(08)	Low
0x20(09)	Low	0x24(10)	Low	0x28(11)	Low	0x2C(12)	Low
0x30(13)	Low	0x34(14)	Low	0x38(15)	Low	0x3C(16)	Low
0x40(17)	Normal	0x44(18)	Normal	0x48(19)	Normal	0x4C(20)	Normal
0x50(21)	Normal	0x54(22)	Normal	0x58(23)	Normal	0x5C(24)	Normal
0x60(25)	Normal	0x64(26)	Normal	0x68(27)	Normal	0x6C(28)	Normal
0x70(29)	Normal	0x74(30)	Normal	0x78(31)	Normal	0x7C(32)	Normal
0x80(33)	Medium	0x84(34)	Medium	0x88(35)	Medium	0x8C(36)	Medium
0x90(37)	Medium	0x94(38)	Medium	0x98(39)	Medium	0x9C(40)	Medium
0xA0(41)	Medium	0xA4(42)	Medium	0xA8(43)	Medium	0xAC(44)	Medium
0xB0(45)	Medium	0xB4(46)	Medium	0xB8(47)	Medium	0xBC(48)	Medium
0xC0(49)	High	0xC4(50)	High	0xC8(51)	High	0xCC(52)	High
0xD0(53)	High	0xD4(54)	High	0xD8(55)	High	0xDC(56)	High
0xE0(57)	High	0xE4(58)	High	0xE8(59)	High	0xEC(60)	High
0xF0(61)	High	0xF4(62)	High	0xF8(63)	High	0xFC(64)	High

Apply   Cancel

1. Port priority is the highest level, don't need to check other QoS attributes is discharged into the highest priority queue if you set the port priority as 1.
2. DSCP priority comes second, unless we do not set DSCP, therefore will check 802.1p priority, otherwise it will line up according to the DSCP settings.

3. As above, the three priority can be used alone, can also be used at the same time, queuing according to the above rules.

6.6 Redundancy
6.6.1 Port Trunking

In telecommunications, trunking is a method for a system to provide network access to many clients by sharing a set of lines or frequencies instead of providing them individually. This is analogous to the structure of a tree with one trunk and many branches. Trunking, is set by the configuration software, the two or more physical ports get together into a logical path to increase the bandwidth between the switch and the network node.

Trunking is a packaging technology, it is a peer to peer link, both ends of the link are switches, it can be a switch and a router, and also can be a host, switch or router. Based on port trunking function that allows between two or more ports between switches, switches and routers, hosts the switch or router connected in parallel to provide for the simultaneous transmission of higher bandwidth and greater throughput, significantly entire network

capacity. Trunking is more economical to increase the bandwidth between the switch and network device, such as servers, routers, workstations, or other switches. Trunking function is to integrate more than one physical port (typically 2-4) to a logical channel.

Current Location>>Main Menu>>Redundancy>>Port Trunking>>Static Trunking

（Figure 6.6.1）

Device supported 4 trunking group, operate method: choice apply,   choice the port need to trunking the port list, Choice setting, available after reboot. If the port already set to Ring port, it can not set to trunking port. Each trunking group at least have 2 port member, at more 4. 1 port can not exit in 2 trunking group

1. The trunking groups require all the attributes can be the same, including speed, duplex, STP state etc.
2. If you do not confirm the STP state, please disable RSTP function, or close others, leaving only one STP channel. 3.Port 1 as the system reserved, can not be used as trunking.
4.The ports of having been set to the port aggregation that can not be set to ring ports.

6.6.2 Rapid Ring

SwRing™ technology provides auto-recovery and reconnection mechanism for broken network. When network is broken, it has link redundancy and self-recovery capability and self-recovery time is less than 20ms. SW-Ring is a technology designed for industrial control network requiring high reliability.

SwRing™ technology support maximum 250 pieces switches, in which the **SwRing™** its self-recovery time is <20ms.
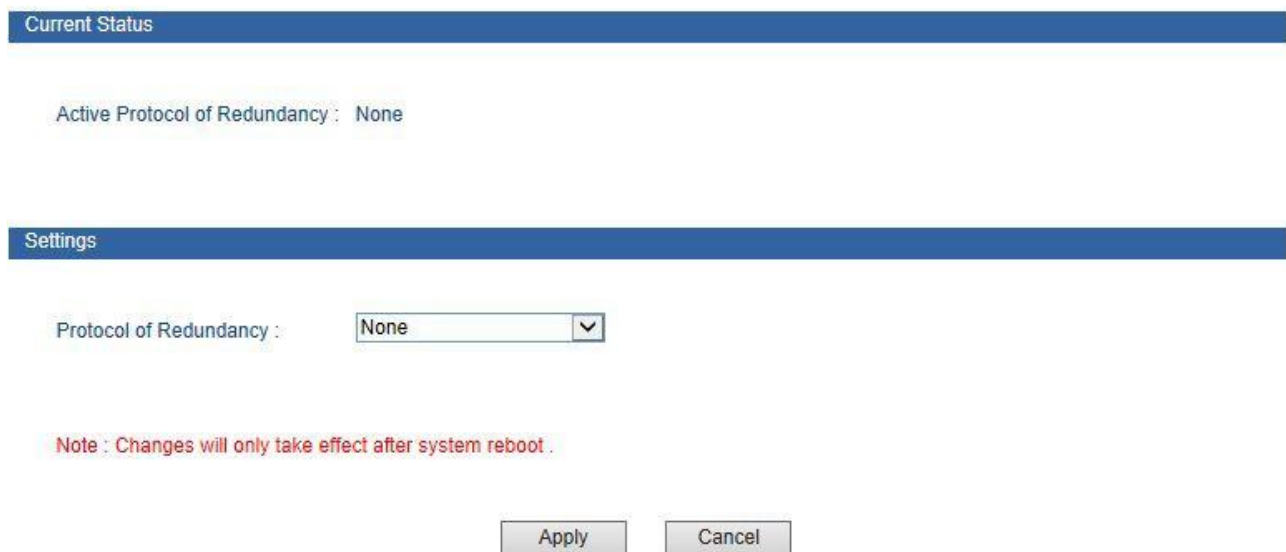
Each port of IT-ES7110-IM-3GS series switch can be Ring Port to connect other switches. When network is broken, relay for failure alarm will be activated. Redundant organization of **SwRing™** enable backup link to recover network instantly.

Self-developed patented technology for SW-Ring network can realize the intelligent redundancy for industrial Ethernet switch, which can make you easily and conveniently establish redundant Ethernet, and can facilitate the quick recovery of any network section of automatic system disconnected from the network. IES7110 series supports maximum 4 ring groups. Each group set up 2 ports as Ring Port and a port cannot belong to several rings.

Hello_time setting is time interval of sending detecting packet to network at regular time. The unit is ms. Its main purpose is to detect network connection. It sends a detecting packet to next door devices by CPU. If they receive it, then reply a confirm packet to ensure network connection is active. If this setting will influence self-recovery time, we suggest advanced users can use it.

Basic interface of Rapid Ring as shown in figure 6.6.2:

Current Location>>Main Menu>>Redundancy>>Rapid Ring

Current Status

Active Protocol of Redundancy :   None

Settings

Protocol of Redundancy : | None ▼ |

Note : Changes will only take effect after system reboot .

| Apply | | Cancel |

（Figure 6.6.2）

Initial interface display redundancy protocol is none, can configure it through [Settings]. There has 3 type SW-Ring arithmetic: Ring V1,Ring V2 and Ring V3), Ring V1 support single ring, Ring V2 support single and coupling ring, Ring V3 Single ring, coupling ring, chain ring and Dual_homing.

1. Method to enabled Ring V1:

　　　　1. Enable Ring V1，Select Ring V1 in [Settings] drop-down menu, figure as 6.5.3

Current Status

Active Protocol of Redundancy :   None

Settings

Protocol of Redundancy :

None
SW-Ring V1
SW-Ring V2
SW-Ring V3
RSTP(IEEE802.1W/1D)

Note : Changes will only take effect after system reboot .

Apply   Cancel

（Figure 6.5.3）

2. After select Ring V1, Interface as figure 6.5.4, Ring V1 just support single ring

Settings

Protocol of Redundancy :   SW-Ring V1 ▾

Port 1 :   1 ▾

Port 2 :   2 ▾

Note : Changes will only take effect after system reboot .

[Apply]   [Cancel]

（Figure 6.5.4）

3,Select "Apply".

2. Method to enabled Ring V1:

1. Enable Ring V2，Select Ring V2 in [Settings] drop-down menu, figure as 6.6.3

Current Location>>Main Menu>>Redundancy>>Rapid Ring

Current Status

Active Protocol of Redundancy :   None

Settings

Protocol of Redundancy :
| None |
| SW-Ring V1 |
| SW-Ring V2 |
| SW-Ring V3 |
| RSTP(IEEE802.1W/1D) |

Note : Changes will only take effect after system reboot .

[Apply]   [Cancel]

（Figure 6.6.3）

2. Enable ring group 1(or group 2), input network ID (support 0-255 pure digital), select the ring port in ring port 1 and ring port 2, figure as 6.6.4

（Figure 6.6.4）

Ring V2 can also set Hello_time . Hello_time setting is time interval of sending detecting packet to network at regular time. The unit is ms. Its main purpose is to detect network connection. This setting will influence self-recovery time, we suggest advanced user use it.

3. Method to enable Ring V2 coupling ring
The architecture of coupling ring as figure 6.6.5

Coupling ring（Figure 6.6.5）

Operation method:

1. Select Ring V2, enable ring group 1 and 2. (Hello_time can be disable, if enable, time of sending Hello packet could not be very fast, it will influence CPU operate speed)；

2. Set 105, 106 device's ring port as port 3 and port 4 in ring group 1, network ID:1, type: single ring. Set ring port as port 6 in ring group 2 , network ID: 2, type: coupling ring, figure as 6.6.6.

（Figure 6.6.6）

3. Set 100, 101 device's ring port as port 3 and port 4 in ring group 1, network ID:1, type: single ring. Set ring port as port 6 in ring group 2 , network ID: 3, type: coupling ring, figure as 6.6.7.

（Figure 6.6.7）

3. Set 107, 108, 109 device's ring port as port 3 and port 4 in ring group 1, network ID: 1, type: single ring. Set 102, 103, 104 device's ring port as port 3 and port 4 in group 1, network ID: 2, type: single ring.

4. Connect 101-104 , 105-109 device's port 3 and port 4 with network cable. Connect 100,101, 105, 106 device 's port 6 with network cable. Figure as 6.6.5

5. Coupling ring can work according to device VLAN, normally 100, 101, 105 and 106 device's VLAN configuration is as figure 6.6.8:

Port:	Port CPU	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port G1	Port G2
VID:1	UnTagged	UnTagged	--	--	--	Tagged	Tagged	--	Tagged	Tagged
VID:2	--	--	UnTagged	UnTagged	UnTagged	Tagged	Tagged	UnTagged	Tagged	Tagged

（Figure 6.6.8）

4. Method to enable Ring V3

1. Enable Ring V3，Select Ring V3 in [Settings] drop-down menu, figure as 6.6.9

（Figure 6.6.9）

2. After select Ring V3, Configuration interface is as figure 6.6.10, we can see Ring V3 support 4 different ring group: Single, Coupling, Chain and Dual_homing.
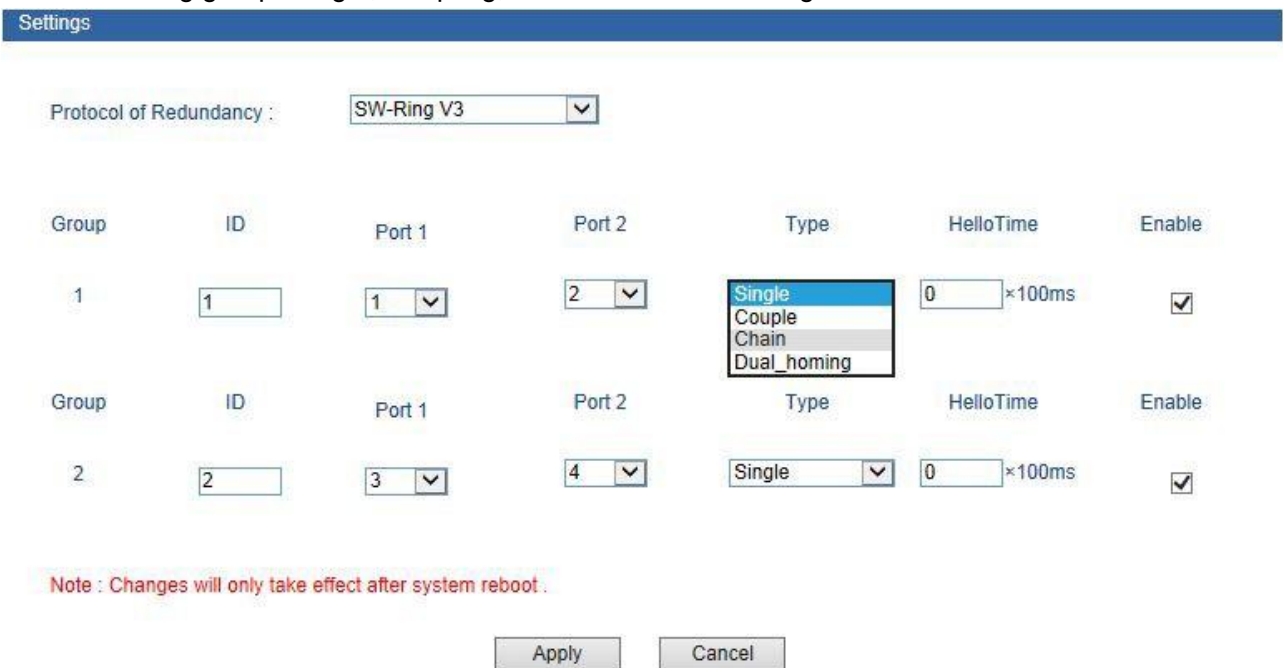
（Figure 6.6.10）

3. Enable Ring Group 1（or Group 2）, and enter into Network ID（support 0-255 number only）.Select Ring Port between Port 1 and Port 2.

"Chain" refers to strengthen user's capability of making any type of redundant topological structure with flexibility by taking an advanced software technology. In fact, Chain is to cascade several switches already set up to Ring and both sides of chain access to network.

"Dual Homing" refers to a fact that two Rings connect the same switch. This type of configuration is ideal choice for centralized management of several Rings.

Method to enable Chain and Dual Homing is similar to that to enable Single Ring and Coupling Ring. It only needs to select corresponding items in [Type].

1. Method to enable Ring V3 coupling ring

The architecture of coupling ring as figure 6.6.11

Coupling（Figure 6.6.11）

Operation method:

1. Select Ring V2, enable ring group 1 and 2. (Hello_time can be disable, if enable, time of sending Hello packet   could not be very fast, it will influence CPU operate speed)；

2. Set 105, 106 device's ring port as port 1 and port 2 in ring group 1, network ID:1, type: single ring. Set ring port as port 4 in ring group 2 , Coupling ctrl port: 2, network ID: 3, type: coupling ring, figure as 6.6.12.

Group	ID	Port 1	Port 2	Type	HelloTime	Enable
1	1	1	2	Single	0 ×100ms	☑

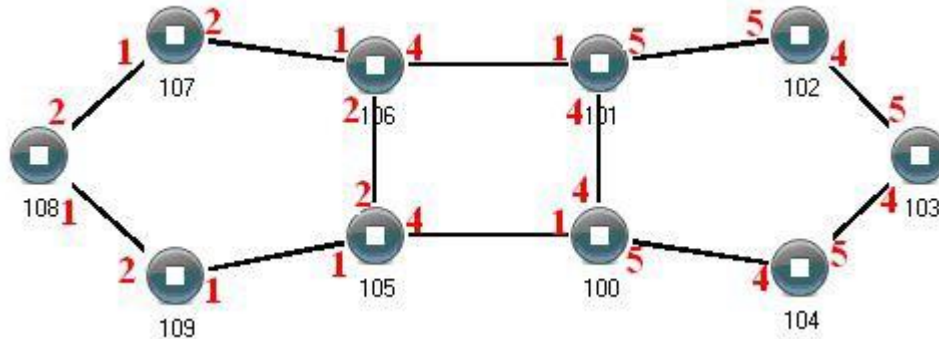| Group	ID	Coupling Port	Coupling Ctrl Port	Type	HelloTime	Enable
2	3	4	2	Couple	0 ×100ms	☑

（Figure 6.6.12）

3. Set 107, 108, 109 device's ring port as port 1 and port 2 in ring group 1, network ID: 1, type: single ring. Set 102, 103, 104 device's ring port as port 4 and port 5 in group 1, network ID: 2, type: single ring. Figure as 6.6.5

4. Connect 101-104 device's port 4 and port 5 with network cable. Connect 105-109 device's port 1 and port 2 with   network cable, Connect 101 device's port 1 to 106 device's port 4 with network cable, Connect 100 device's port 1   to 105 device's port 4 with network cable.

5. Coupling ring can work according to device VLAN, normally 100, 101, 105 and 106 device's VLAN configuration is as figure 6.6.8:

Group	ID	Port 1	Port 2	Type	HelloTime	Enable
1	2	4	5	Single	0 ×100ms	☑

Group	ID	Coupling Port	Coupling Ctrl Port	Type	HelloTime	Enable
2	3	1	4	Couple	0 ×100ms	☑

（Figure 6.6.13）

2. Method to enable Ring V3 Chain ring
The structure of Chain ring as figure 6.6.14
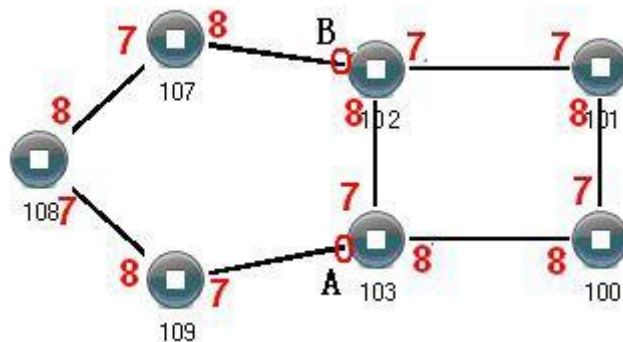
Chain (Figure 6.6.14)

Operating method:

2. Enable Ring Group 1: Hello time can be disable too, if it enable, time of sending Hello packet could not be very fast, or it will influence CPU dealing speed.
3. Set up Port 7 and 8 of Device 100, 101, 102 and 103 to be Ring Port in Ring Group 1, Network ID is1, Ring Type is Single; as shown in figure 5-47. Set up Port 7 and 8 of Device 107, 108 and 109 to be Ring Ports in Ring Group 2, Network ID is 2. Ring Type is Chain; as shown in figure 6.6.16.

Group	ID	Port 1	Port 2	Type	HelloTime	Enable
1	1	7	8	Single	0 ×100ms	✓

（Figure 6.6.15）

Group	ID	Port 1	Port 2	Type	HelloTime	Enable
1	2	7	8	Chain	0 ×100ms	✓

（Figure 6.6.16）

4. Use a wire to connect Port 7 and 8 of Device 107-109 in turn to make a chain. Use a wire to connect Port 7 and 8 of Device 100-103 in turn to make a Single Ring, Then use a wire to connect Port 8 of Device 107 and Port 7 of Device 109 to normal port of Device 102 and 103. Chain is finished.

⚠️

> 1. Port can not be trunking setting when it is already Ring port.
> 2. In the same single ring, identity must be consistent, otherwise it will not built a ring and can not communicate.
> 3. All ring ports in the VLAN settings must be TRUNK tagged VLAN member, otherwise can not communicate.
> 4. To form tangent ring or other complex rings, should pay attention to the ring identity whether is it consistent, different   single ring identification must be different.

6.6.3 RSTP

The first spanning tree protocol was invented in 1985 at the Digital Equipment Corporation by Radia Perlman. In 1990, the IEEE published the first standard for the protocol as 802.1D,based on the algorithm designed by Perlman. Subsequent versions were published in 1998 and 2004, incorporating various extensions.

Although the purpose of a standard is to promote interworking of equipment from different vendors, different implementations of a standard are not guaranteed to work, due for example to differences in default timer settings. The IEEE encourages vendors to provide a "Protocol Implementation Conformance Statement", declaring which capabilities and options have been   implemented,[8] to help users determine whether different implementations will interwork correctly.

Also, the original Perlman-inspired Spanning Tree Protocol, called DEC STP, is not a standard and differs from the IEEE version in message format as well as timer settings. Some bridges implement both the IEEE and the DEC versions of the Spanning Tree Protocol, but their interworking can create issues for the network administrator, as illustrated by the problem discussed   in an on-line Cisco document.[9]

Rapid Spanning Tree Protocol

In 2001, the IEEE introduced Rapid Spanning Tree Protocol (RSTP) as 802.1w. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new   convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards- compatible with standard STP.While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within 3 × Hello times (default: 3 times 2 seconds) or within a few milliseconds of a physical link failure. The so-called Hello time is an important and configurable time interval that is used by RSTP for several purposes; its default value is 2 seconds. Standard IEEE 802.1D-2004 incorporates RSTP and obsoletes the original STP standard Select RSTP function in rapid ring network interface as

Settings

Protocol of Redundancy :

None
SW-Ring V1
SW-Ring V2
SW-Ring V3
RSTP(IEEE802.1W/1D)

Note : Changes will only take effect after system reboot .

Apply   Cancel

Current Status

Active Protocol of Redundancy : None

Settings

Protocol of Redundancy :   RSTP(IEEE802.1W/1D) ▼

Bridge Priority :   32768 ▼

Hello Time(s) :   2   (1~10)   FWD Delay(s) : 15   (4~30)

MAX Age(s) :   20   (6~40)   RSTP Status :   RSTP Port Information

Port	Cost	Priority	P2P	Edge	Port STP
1	0	128 ▼	Auto ▼	☐	☐
2	0	128 ▼	Auto ▼	☐	☐
3	0	128 ▼	Auto ▼	☐	☐
4	0	128 ▼	Auto ▼	☐	☐
5	0	128 ▼	Auto ▼	☐	☐
6	0	128 ▼	Auto ▼	☐	☐
7	0	128 ▼	Auto ▼	☐	☐
8	0	128 ▼	Auto ▼	☐	☐
G1	0	128 ▼	Auto ▼	☐	☐
G2	0	128 ▼	Auto ▼	☐	☐

Note : Changes will only take effect after system reboot .

（Figure 6.6.17）

Rapid Spanning Tree of concepts:

Switch priority：As the bridge priority，the bridge priority and bridge MAC address combine bridge ID,the smallest ID bridge will become the root bridge on the network.

Polling interval：how often send BPDU packet at one time.

Forwarding delay：the port state of switch remain a forward delay time over the listening and learning.

The maximum aging time：after one switch receive a packet from other switches , how long the packet is valid.

The port concepts of RSTP**:**

Port path overhead：port link cost compared with port priority and port ID .

Port priority：port priority among the net bridge compared with port priority and port ID

Point to point network connection：directly connect with switches port each other ,the port is P2P, which adopted negotiation mechanism,RSTP can achieve port state rapid conversion RSTP

Directly connect terminal：connect the edge of network switch with terminal devices with **configuration Edge port**，which can achieve port state rapid conversion without the processing Discarding， Learning，Forwarding

Don't join RST structure：don't participate in RSTP running

RSTP switch port states:

1. **Blocking**- A port that would cause a switching loop if it were active. No user data is sent or received over a blocking port, but it may go into forwarding mode if the other links in use fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state. Prevents the use of looped paths.

2. **Listening**- The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. It does not populate the MAC address table and it does not forward frames.

3. **Learning**- While the port does not yet forward frames it does learn source addresses from frames received and adds them to the filtering database (switching database). It populates the MAC Address table, but does not forward frames.

4. **Forwarding**- A port receiving and sending data, normal operation. RSTP still monitors   incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

The example of Configuration: The priority of network bridge is "32768"，If there did not have network ID less than itself, itself is root network bridge. There did not have same network ID in network. Every 2 seconds, the network bridge will transmit BPDU message to all appoint port. If did not receive BPDU message more than

20 seconds, it realized port invalid, will calculate the status of network bridge again. Each status exchange for each other if need to transmit, need to wait 15 seconds.

6.7 Access   Profile
6.7.1   Login
Settings

Enterprise usually required two different person to monitor device and manage system/ network . The authority need to separate. Monitor person was in charge of monitor work, system/network person was in charge of system/work management. The switch provided classification management: Administrator authority   and Observer authority. Observer just had authority to check the status of switch. Administrator had   the authority to configure the parameters of the switch.

Index

User index indicates which group of users. There are three user indexes in drop-down list.

Access level:

administrator： have   the   right   to   check   and   configure   all   settings

observer：have the right to check all settings merely

Login name

The identity of visitor with the letter combination is no more than 16 bytes

Password:

Visitor use password, user authority allows the letter combination no more than 16 bytes

Confirm password

Make sure the last time input password is correct.

Index : 1

Access Level : Administrator

Login Name : admin

Password : ••••••••

Confirm Password : ••••••••

48

Apply   Cancel

Index : 2

Access Level : Observer

Login Name : guest

Password : ••••••••

Confirm Password : ••••••••

Apply   Cancel

（Figure 6.7.1）

1.Please contact our online technical support if you forget login name and password
2. Set same user mane, the front settings of user name/password will be available.

User must remember user name and password after modified. If forget it, please use DIP switch to make default factory. The   default user name and password: admin.

6.8 Remote monitoring

6.8.1 SNMP management

1. Introduction of SNMP

SNMP (Simple Network Management Protocol) is an internet-standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

2. Work Mechanism of SNMP

SNMP includes 2 parts: NMS and Agent:

NMS: Network Management Station. Software runs on the manager. The common management platforms are "Quid View", "Sun Net Manager" and "IBM Net View". Agent is the software of the server running in the network device.

NMS can send "Get Request", "Get Next Request" and "Set Request" message to Agent. After Agent gets those messages, it will read or write according to the message type to create Response message and send the Response message back to NMS. Agent will also send Trap message to NMS when the device is abnormal.

3. SNMP Version

Currently SNMP Agent of the device supports SNMP V3 and it is also compatible with SNMP V1and SNMP V2C. It is authenticated by user name and password in SNMP V3.

SNMP V1 and SNMP V2C adopt authentication of Community Name. The SNMP message of the community name which is not authenticated will be discarded. SNMP community name defines the relationship of SNMP NMS and SNMP Agent. User can choose the following one or more features related to community name.

1. Defines MIB view of community name.

2. Setup visit privilege of MIB objective is Write or Read. Community name with Read privilege can   check the device information only. Community name with Write privilege can configure the device.

3. Setup appointed basic visit control list of the community name.

IT-ES7110-IM-3GS series supports SNMP V1/V2c. Both SNMP V1 and V2c use public character strings for match authentication.

SNMP usually uses UDP Port 161(SNMP) and 162 (SNMP-traps) based on TCP/IP protocol. SNMP protocol agent is existed in network device. MIB (information specific to the device) is uses as device connector. These network devices can be monitored or controlled through the agent. When trap event happens, a message is transmitted by SNMP Trap, an available trap receiver can get this trap information.

SNMP supports 3 kinds of basic operating in total:

Get: Manager can use this to get some variable value of Agent. **Set:** Manager can use this to set up some variable value of Agent. **Trap:** Agent uses this to send an alarm to manager.

（Figure 6.8.1）

Curect Location>>Main Menu>>Remote Monitoring>>SNMP Configuration

SNMP Configuration :	⦿ Enable ○ Disable
SNMP V1/V2 :	
SNMP Read Community :	public
SNMP Read/Write Community :	private
SNMP Gateway :	192.168.1.1

50

Apply   Cancel

Read Community
Use a character string to name a SNMP community. This community only has Get privilege.
Read/Write Community
Use a character string to name a SNMP community. This community has Get and Set privilege.
SNMP TRAP Gateway
IP address of the receiver of the alarm information sent Agent

The device supports warm start of Trap. If existed IP address in Trap gateway, click "Apply", the Trap receiver can get the trap information. If the trap receiver cannot get trap information, please check network setting and connecting. Please pay attention to the privilege of Read and Write in SNMP Explorer.

6.8.2 Relay Alarm

Warning had 2 type: Power alarm, port alarm. Main function: once the devices were in unusual status, can inform administrator in time and repair the status of device quickly, can avoid more lose
Relay warning input type: Close/Open. Once select Close, the light will be bright when have alarm. Relay will be in open status.

Power alarm
IT-ES7110-IM-3GS series provided dual DC power supply (AC power supply did not have alarm), if one power supply had problem, another will support power supply immediately, dual power supply hot back-up. Select to enable power alarm, If power supply was in unusual status, device will send alarm signal, inform power supply work unusual.

Port Alarm
Alarm when port disconnect. Enable port alarm, if port was in unusual status(Connect or disconnect), device will output a signal, inform the device work unusual.

（Figure 6.8.2）

⚠️

In default status, the type of relay output is open, the alarm light is OFF, have no alarm, relay alway open.   When the device have alarm, the light is ON, relay close

6.9 Traffic Statistics

The function of traffic Statistics is to calculate the data packets in a fixed time, included transmit and receive data packets.

Operate method: Start to calculate after select clear

6.9.1 RX frame statistics

Frame Name	Description
InUnicasts	Valid Unicast Data Frames
InBroadcasts	Valid Broadcast Data Frames
InPause	Number of Valid Flow Control Pause frames
InMulticasts	Valid multicast excluding InBroadcasts
InFCSErr	Number of FCS checkout error frames (completed data)
AlignErr	Number of FCS checkout error frames (uncompleted data)
InGoodOctets	Number of valid received data byte (including FCS)
InbadOctets	Number of invalid received data byte (including FCS)
Undersize	Number of valid data frames less than 64 bytes
Fragments	Fragments (less than 64 bytes, invalid FCS)
In64Octets	Number of frames with 64 bytes (including invalid frames)
In127Octets	Number of frames between 65 and 127 bytes (including invalid frames)
In255Octets	Number of frames between128 and 255 bytes (including invalid frames)
In511Octets	Number of frames between 256 and 511 bytes (including invalid frames)
In1023Octets	Number of frames between 512 and 1023 bytes (including invalid frames)
InMaxOctets	Number of 1024-1518 or 1522 bytes（802.1Q） (including invalid frames)

Jabber	Invalid oversized frames received (more than 1518 or 1522)
Oversize	Valid oversized frames received (more than 1518 or 1522)
InDiscards	Number of Valid discarded frames (because of cache, flow control, etc.)
InFiltered	Valid frames filtered (because of VLAN and so on)

6.9.2 TX frame statistics

OutUnicasts	unicast data frames output
OutBroadcasts	Broadcast data frames output
OutPause	Number of output flow control pause frames
OutMulticasts	Multicast data frames output
OutFCSErr	Invalid FCS frames output
OutOctets	Number of output bytes（including FCS）
Out64Octets	Number of output frames with 64 bytes
Out127Octets	Number of output frames between 65 and 127 bytes
Out255Octets	Number of output frames between 128 and 255
Out511Octets	Number of output frames between 256 and 511
Out1023Octets	Number of output frames between 512 and 1023
OutMaxOctets	Number of output frames between 1024 and 1518 or 1522 bytes（802.1Q）
Collisions	Number of collision in output
Late	Number of collision after frames output 64 bytes
Excessive	Number of unsuccessful output frames（trying more
Multiple	Number of successful output frames（collision more than 1 time）
Single	Number of successful output frames（collision happens
Deferred	Number of successful output frames（the receiver is busy, but It sends successfully after a delay）
OutFiltered	Filtered frames output
OutDiscards	Discarded frames output（because of cache, flow control, etc.）

6.10 Diagnosis

6.10.1 Mirror

Port mirroring refers to copy data from the port which need to be monitored to appointed monitoring port for analysis and monitoring. Ethernet switch supports many-for-one mirror which means messages from several ports can be copied to a monitored port. User can appoint the direction of monitored message, such as only monitoring of transmitted messages of appointed port. The device configures port mirroring function through port mirroring group. Each group includes a monitored port and a group of mirror ports. Total bandwidth of mirroring is not more than that of monitored port. It is good to monitor and manage its internal network data when using

port mirroring in a company. It is also good to locate the failure when network is cut up.

Operating method: Enable port mirroring, select monitored port, select mirror port. Monitored port can get data from mirror port and select monitored data at last: all data or egress data. Select Apply. As shown in figure 6.10.1,6.10.2

（Figure 6.10.1）

（Figure 6.10.2）

Mirror Port

It defines a group of ports which are needed to be monitored. The device collects data from these ports.

Monitored Port

It defines a group of ports which are used to monitor other ports. The device outputs the data through these ports.

Watch direction

This parameter indicates the direction of the data. It includes 3 kinds of choices: "All", "Ingress" and "Egress".

1. This function is not often used. Otherwise other port-based higher management function like RSTP,IGMP SNOOPING
2. Port mirroring function can only deal with the normal FCS packets. It cannot deal with error data frames.

6.11 Basic settings

6.11.1 Device address

Device configuration support two modes, DHCP and static IP address, can get the device's IP address via client when the DHCP function is running, if you need NTP that need to connect internet, please enter the available and correct gateway and DNS address.

IP Address

IP address is a address of 32 bits length which is assigned to the device on the internet. The IP address consists of two fields: the network number field (net-id) and the Host ID field (host-id). For can conveniently manage IP address, IP addresses are divided into five categories. As blow：

Network type	Address range	Available IP network range
A	0.0.0.0～126.255.255.255	1.0.0.0～126.0.0.0
B	128.0.0.0～191.255.255.255	128.0.0.0～191.254.0.0
C	192.0.0.0～223.255.255.255	192.0.0.0～223.255.254
D	224.0.0.0～239.255.255.255	Non
E	240.0.0.0～246.255.255.255	Non
Others	255.255.255.255	255.255.255.255

A, B, C class address is unicast address; D class address is multicast address; E class address is reserved

to prepare for the future for special purposes.

IP address using dotted decimal. Each IP address is represented as four decimal integers separated by decimal   points, each integer corresponds to a byte, such as, 10.110.50.101.

Subnet Mask

Mask is corresponding 32 bits number of IP address. Some are 1, the others are 0. These 1 and 0 can be combined arbitrary in principle, but the first continuous bits are 1 when designing subnet mask. IP address can be divided into 2 parts by subnet mask: subnet address and host address. 1 in IP address and subnet corresponds to   subnet address, other bits are host address. A type of address corresponding mask is 255.0.0.0; mask of B type   address is 255.255.0.0; mask of C type address is 255.255.255.0.

Default Gateway

Default gateway in the host PC is generally called default route. Default route refer to a kind of router that destination address of IP data packet will choose when it don't find other existing route. All data packets of destination address which don't exist in the list of router will choose default route.

DNS Address
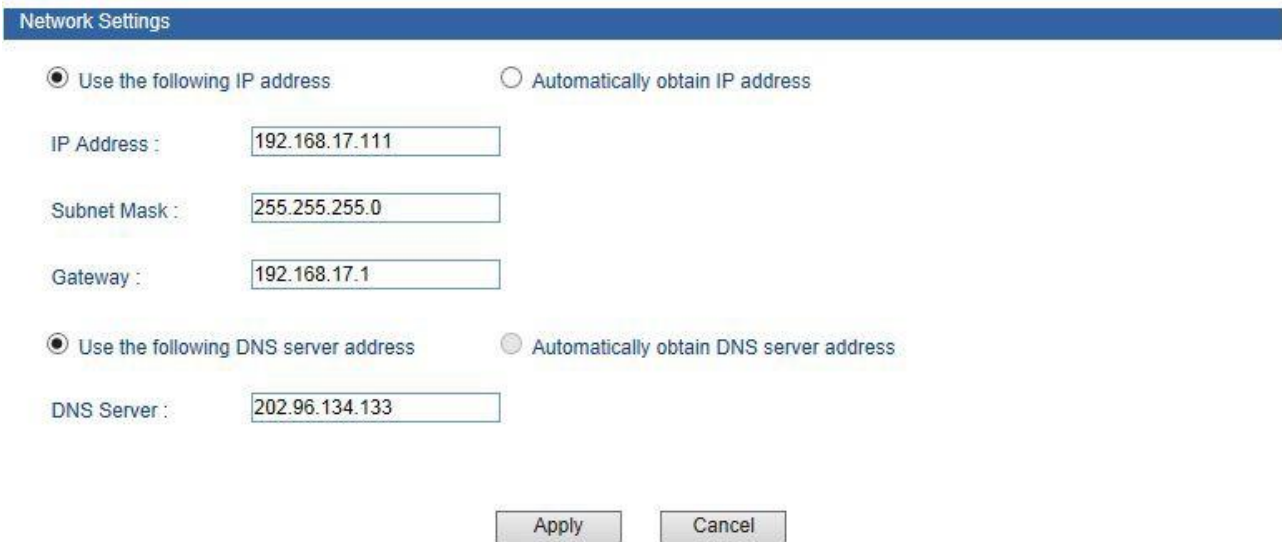
DNS (Domain Name Server) is for us to analyze domain to IP address of the Internet. If our equipment needs to access a host, you need to use this server to resolve an IP address.

Device reboot

Can reboot the switch remote. Knock [Basic settings/Network&reboot] menu, Enter into reboot interface, Figure as 6.11.1.

Knock<Reboot> button, after confirmation, device will be reboot. After 20 seconds, know menu bar and back to WEB managed login interface.

Current Location>>Main Menu>>Basic Settings>>Network & Reboot

Network Settings

- ◉ Use the following IP address   ○ Automatically obtain IP address

IP Address :   192.168.17.111

Subnet Mask :   255.255.255.0

Gateway :   192.168.17.1

- ◉ Use the following DNS server address   ○ Automatically obtain DNS server address

DNS Server :   202.96.134.133

[Apply]   [Cancel]

Device Reboot

[Reboot]

（Figure 6.11.1）

⚠️

| Before reboot, please save all configurations. Otherwise, all configuration will be lost |

6.11.2 System identification

In System Identification interface we can see Model, Name, Description, Serial NO., and Contact Information. We can modify these above items by this function. It will take effect after system reboot. Figure

6.11.13 is initial device settings of IT-ES7010-IM-2GS series switch.

Settings

Module : MangedSwitch

Name : IndustrialSwitch

Description : 10PORT

Serial No. :

Contact Information :

Apply   Cancel

（Figure 6.11.3）

Name
To give a name to each device, length is not more than 16 bytes.

Description
A brief description to a device, the length is not more than 16 bytes.

Serial No.
Display Installation Location of the device, the length is not more than 30 bytes.

6.11.3 System File Upgrade

The menu included 5 functions: Factory default, Device reboot, Download Configuration, up load configuration, upgrade firmware.

Current Location>>Main Menu>>Basic Settings>>System File Update

Factory Default

Load Factory Default :   OK

Device Reboot

Reboot

Update Configuration File from Local PC

Download Configuration :   [Download]

Upload Configuration :   [_____] [Browse...] [Upload]

Upgrade Firmware from Local PC

Upgrade Firmware :   [_____] [Browse...] [Upgrade]

1. Factory Default
If you know the IP address of the device, user name and password:
Use IE to login Web interface.
Click "System Management" Click
"System File Update" Choose
"Factory Default" Click "OK"
Notice: the IP address will be "192.168.1.254".
Open a new interface, input "192.168.1.254" to make a new configuration.

2. Reboot
Click "OK", the device reboot. Before reboot, please save all configuration, otherwise the unsaved
configuration would be lost after reboot.

3. Download Configuration
If you know the IP address of the device, user name and password:
Use IE to login Web interface.
Click "System Management" Click
"System File Update"
Choose "Download Configuration" Click
"Download"
Choose the name of the file and the place to save.

4. Upload Configuration
If you know the IP address of the device, user name and password:
Use IE to login Web interface.
Click "System Management" Click
"System File Update" Choose "Upload
Configuration" Click "Upload"

5. Upgrade Firmware
If you know the IP address of the device, user name and password:
Use IE to login Web interface.
Click "System Management"

Click "System File Update" Choose
"Upgrade Firmware"
Click "Browse" and find the place of uploading the file. Click
"Upgrade"
A suggestion" interruption of power is not allowed during uploading" , confirm it.

1.Load factory default will result in all status be in factory default settings, the IP could be static IP address "192.168.1.254".　2.Upload the configuration file, in the new configuration if static IP is not in the same network segment, the website will not　be opened.

3.Use dynamic IP settings, but there is no DHCP server on the network segment, that will result in the relevant part of the IP　will not be updated in the new configuration when upload configuration.

58

CHAPTER 7 Function setting

7.1 DIP switch

IT-ES7110-IM-3GS series have 4 DIP switch. Can default factory through DIP 2

DIP switch	ON
1	Hold
2	Factory default
3	Hold
4	Hold

7.1.1 Default factory

Put the DIP switch 2 to ON, Power ON again, the default factory finished. After default factory, must put the DIP switch to OFF, otherwise, will default factory again when power ON next time.

⚠ :

Except DIP switch 2 need to put ON when default factory. Other DIP switches must always in OFF status, otherwise, the device may work unusual

Chapter 8 Repair and Service

The company provides a five-year product warranty, from the date of shipment. According to the product specifications, during the warranty period, the company will be free to repair or replace the product if the product has any failure or operation fails. However, these commitments do not cover damage caused by improper use, accident, natural disaster, improper operation or incorrect installation.

To ensure that consumers benefit from our managed series switches, try to get help in the following ways:

nternet service.

Make a call to our technical office. Return or

replace product.

7.1 Internet Service

Please visit https://www.intellisystem.it

7.2 Make a call to our technical office

You can call our technical support office, the company has professional technical engineers to answer your questions and help you resolve your problems at the first time.

7.3 Repair or Replace

Please to confirm with our technical staff if your product need to repair, replace or return, and then contact our sales man to get a deal with the problem. The above should be in accordance with the company's handler to negotiate for treatment with our technical and salesman to complete the repair, replacement or return.

Appendix 1 Glossary table

	Glossary	Description
A	ARP (Address Resolution Protocol)	An IP address to physical address protocol
	Auto-Negotiation	Switches at both ends of the device in accordance with the maximum performance to auto-negotiate the speed and duplex
B	Broadcast Storm	A port send excessive broadcast frame meantime on the network, accumulate the respond to send messages on the network , consume too much network resources or cause the network
	Broadcasting	A forwarding way send data to all branch of network
C	CoS（Class of Service）	namely 802.1p priority program, CoS offer a way for data packets to join priority tag, classify packets into 8 level with the value 0~7 range
D	DHCP （Dynamic Host Configuration Protocol）	Information for the network to assign dynamically IP address, subnet mask and gateway
	DSCP（DiffServe Code Point）	Packaged in IP packet header of 6 bit domain, can classify packets into 64 level with the value 0~63 range
E	Ethernet	Ethernet uses a bus or star-shaped topology and supports transmission rates up to 10Mbps orders of magnitude. A new version called fast Ethernet speeds of up to 100Mbps
F	Flow Control	Flow control allows low-rate devices communicate with high-rate, the flow control can match high rate port contracting speed with low rate port reception speed according to the way of high rate port pause contract
	Frame	Packets contain the header and tail message of physical media
	Full-Duplex	Receive and send data in progress at one moment meantime on IEEE802.3x standard
H	Half-Duplex	Receive or send data in one direction at one moment in progress on Backpressure standard.
I	IGMP （Internet Group Management Protocol）	Define the mechanism among hosts and three layers multicast device to establish and maintain the relationship between multicast
	IEEE 802.1p	Add the priority network traffic on MAC sub layer of data link layer.
	IEEE 802.1q	Define the VLAN bridge operation。To manage ,define and operate
Q	QoSQuality of Service）	A technology to resolve the network delay and block problems and so on.
T	Trunking	To make an aggregated group tied up a group of ports together to increase bandwidth and improve the connection reliability.
	ToS （Type of Service）	Packaged in IP packet header of 8 bit domain to perform the different priority packets
U	UDP （User Datagram Protocol）	Face to disconnected unreliable transmission layer protocol
	UTP(Unshielded Twisted Pair)	Not shielded media out of twisted pair

Appendix 1 Default factory

Main Menu	Tag	Function	Main Menu
System status	System information	Name	IT-ES7110-IM-3GS
		Module	IT-ES7110-IM-3GS
		Description	Intellisystem
		Serial No.	
		Contact information	marketing@intellisystem.it
Port configuration	Port configuration	Port enable	Enable
		Speed mode	Consult automatic
		Flow control	enable
	Bandwidth management	Egress	No cofiguration
		Ingress	No cofiguration
	Storm suppression		No cofiguration
L2 feature	QoS	802.1p priority	Disable
		Port priority	Disable
		DSCP priority	Disable
	VLAN	802.1Q VLAN	Disable
		Based on port VLAN	Enable
	IGMP		Disable
	Static Unicast FWD		Disable
Redundancy	Port Trunking		Disable
	Rapid Ring	Ring V1	Disable
		Ring V2	Disable
		Ring V3	Disable
	RSTP		Disable
Port Statistics	Traffic		
Diagnosis	Mirror		Disable
Remote Monitoring	SNMP		Disable
	Relay alarm		
System management	Device management	IP	192.168.1.254
		Subnet mask	255.255.255.0
		Default gateway	192.168.1.1

Appendix 3 Treatment of common problem

1. Why the page is not normal when configured by a web browser?
Before the access to WEB interface, please clear the IE cache and cookies. Otherwise, the WEB interface may be not normal.

2. How to do if you forgot password?
You can load factory default to get the initial password if forgot the password, the exact method you can search in the management software. The initial user name and password is "admin".

3. Whether the effects are equivalent that make the configuration via web and by the management software?
Configuration of both is the same, are not in conflict.

4. What kind of alarms will be informed to technical except displayed in the management software?
The computer buzzer of monitoring host will continue to make alarm sound when got alarm information.

5. Why can not increase the bandwidth after configured trunking?
Check the Trunking Port's properties are coincident, including rate, duplex mode, VLAN etc.

6. How to deal the problem that some of ports can not access?
When some of ports can no access, that may be line fault, network card failure and switch port failure, by the following test to find faults:
1. Only change a new Ethernet cable.
2. Use the same Ethernet cable and switch port, to replace the computer.
3. Use the same Ethernet cable and computer, to access other ports.
4. If have confirmed switch fault, please contact manufacture to repair.

7. What about the order of port adaptive status detection?
Port to detect the status in the following order: 100Mbps full duplex, 100Mbps half duplex, 10Mbps full-duplex, 10Mbps half duplex, in descending order to detect and automatically connect with the highest speed.